Security is Just Another Word without Collective Intelligence

2013

DS Benbow, VP Marketing

DS BENBOW CLIFF NOTES
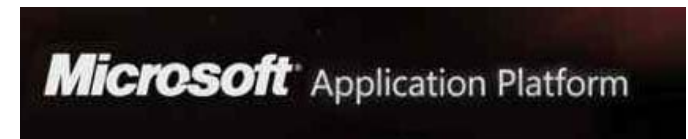
- Lots of startups! (OK only 4)
- Early career: Market Analyst

ABOUT INTERNET IDENTITY

LOCATION	Tacoma, Washington
FOUNDED	1996
WEBSITE	www.internetidentity.com
CUSTOMER FOCUS	Fortune 2,000, financial services, major internet brands, defense, critical infrastructure
THOUGHT LEADERSHIP	**FCC**: Communication, Reliability and Interoperability Council **APWG**: Anti-Phishing Working Group **ICANN**: Security and Stability Advisory Committee **OTA**: Online Trust Alliance **FIRST**: Forum of Incident Response and Security Teams **MAAWG**: Messaging Anti-Abuse Working Group

Cyberattacks continue to increase in terms of sophistication, organization, and destructive impact…

"In the past 18 months, a string of highly sophisticated and targeted cyber attacks across the globe has revealed a seismic shift in the threat landscape." 2011 RSA CISO Report

"Big Data Emerges as a Security Tool" GRT

"What's being stolen? Personal identities, money from banks, blueprints for next-generation jobs. Some estimates put the value of information hacked at up to $US400 billion every year." Article: Almost all US networks can be hacked: Intelligence Committee

"NSA Director on Cyberattacks- 'Everybody's Getting Hit'" ABC News

- Actionable intelligence matters (not data)

- Faster intelligence equals better protection (speed kills)

- Crowdsourcing equals greater efficacy than silos (collaboration = good)

Threat data   Collaboration

CURRENT LANDSCAPE: THE BATTLE IS ASYMMETRICAL

Antivirus software powerless to stop data breach attacks. CIO.com, 2/9/12

DNSChanger infected half of Fortune 500 in 2012
Computerworld, 2/2/12

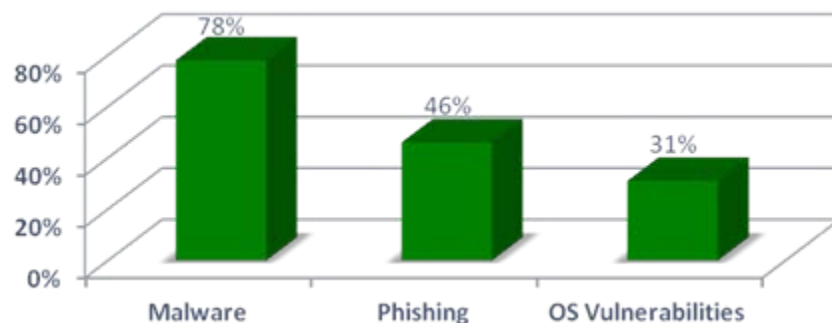**Cost of data breaches averages $7.2M, or $214 per customer record** per Ponemon Institute, The Atlantic, 2/16/12

…91 percent of cyber attacks begin with a "spear phishing" email…computerworld.co.nz/, Dec 2012
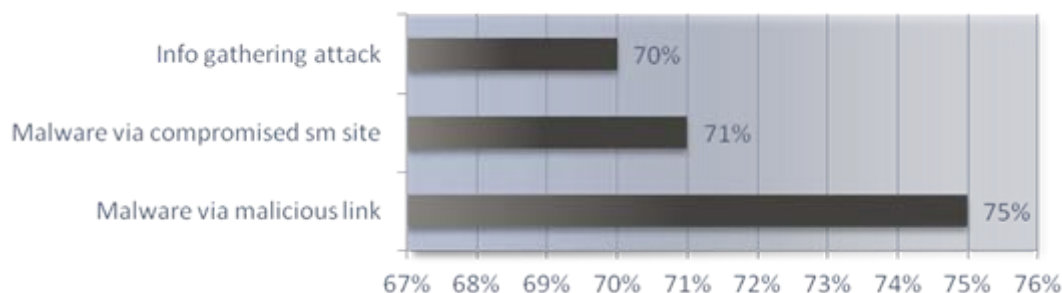

Cyber crime is a permanent part of the Internet tapestry—it's here to stay

MORE OBLIGATORY DATA POINTS

Top Causes for Security Breaches in 2011

Top 3 Types of Threats Posed by Social Media in 2011

Dealing with rampant malware is time and resource intensive

WHAT'S IMPORTANT TO IT SECURITY

The #1 most important metric in determining value of a particular security investment:

Reduction in incident response time   NO

Decline in amount of network downtime   NO

Better risk management strategies   NO

Decline in breaches   NO

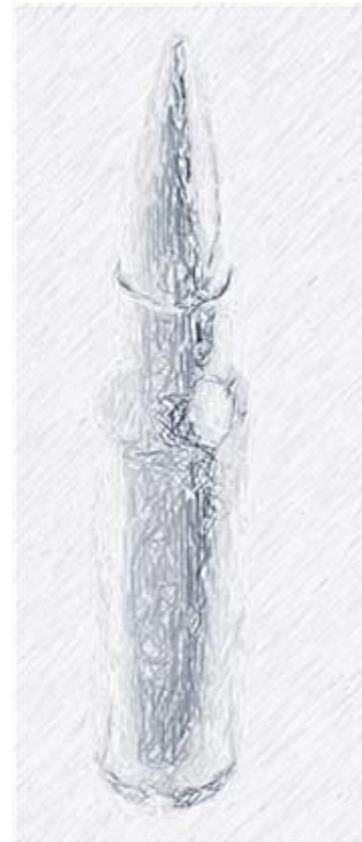Better protection of customer   NO
records/intellectual property

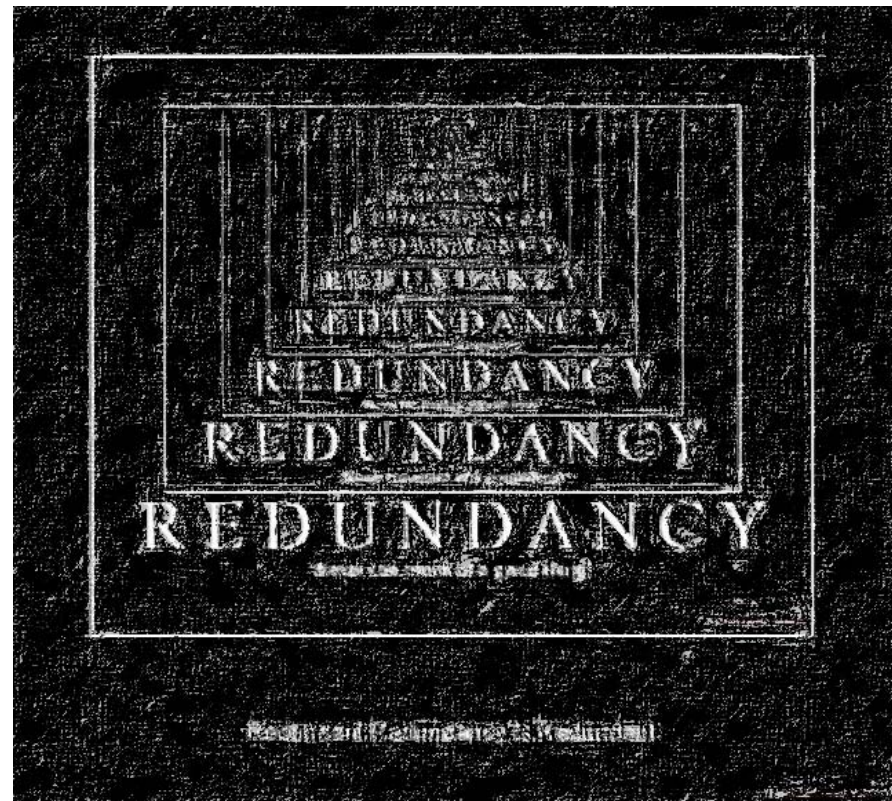**Fewer man hours spent on security-related issues: YES!**

There is no **single** point solution to cybercrime
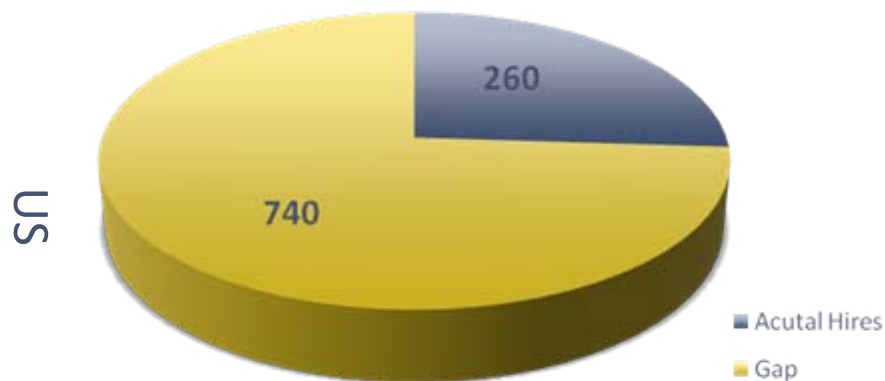

Heuristics vs. **Signatures** is a false argument

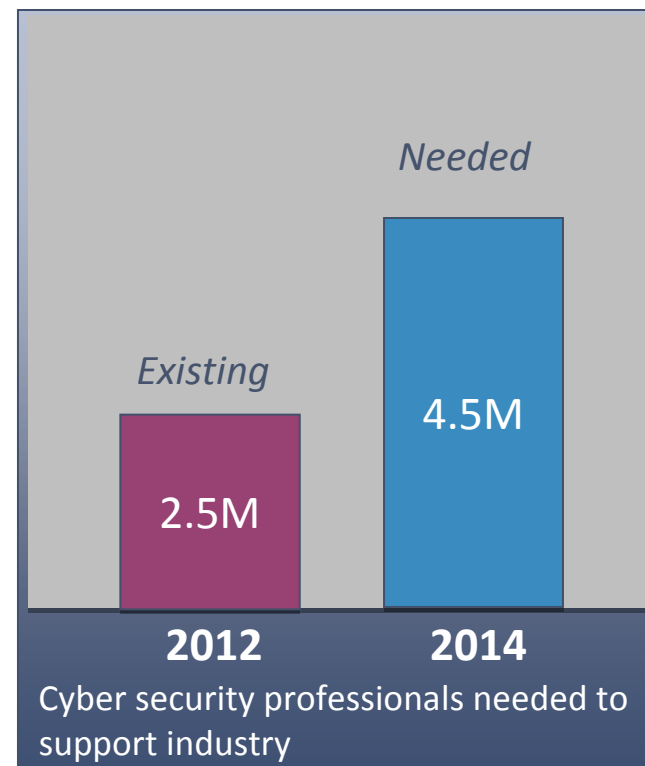Most orgs don't have access to **_known knowns_** and waste cycles determining what's already been determined

HUMAN RESOURCE SHORTAGE

Department of Homeland Security

US

- Acutal Hires
- Gap

In 2009, the DHS announced plans to recruit 1,000 cyber professionals over three years. As of 2011, DHS had only managed to hire about 260.

Globally

Needed

Existing

4.5M

2.5M

2012   **2014**

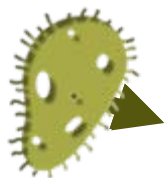Cyber security professionals needed to support industry

The new model needs to highly leverage human capital

http://www.darkreading.com/security/news/240001380/federal-officials-say-cybersecurity-is-greatest-high-risk-skill-gap.html

http://www.cnas.org/csmonitor-cybersecurity-kristin-lord-jacob-stokes

Current silo approaches are costly …

Enterprise **A**

Enterprise **B**

Enterprise **C**

The lack of shared learning creates efficiency for bad actors

It is truly maddening to see examples of bad guys sharing data, tricks, methods and good guys having no effective way of doing it

Anton Chuvakin, Gartner Research Director

BLACKHOLE EXPLOIT

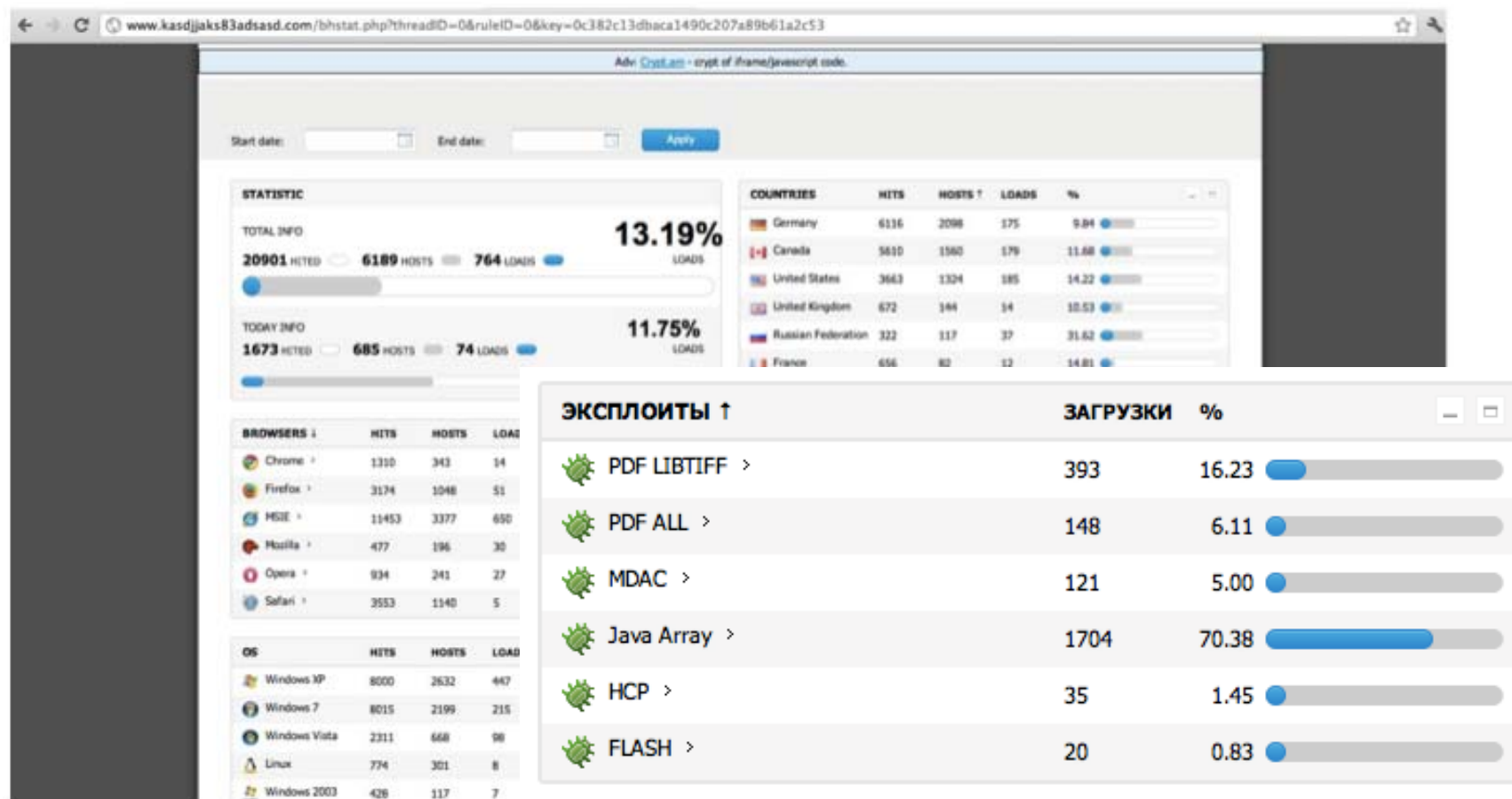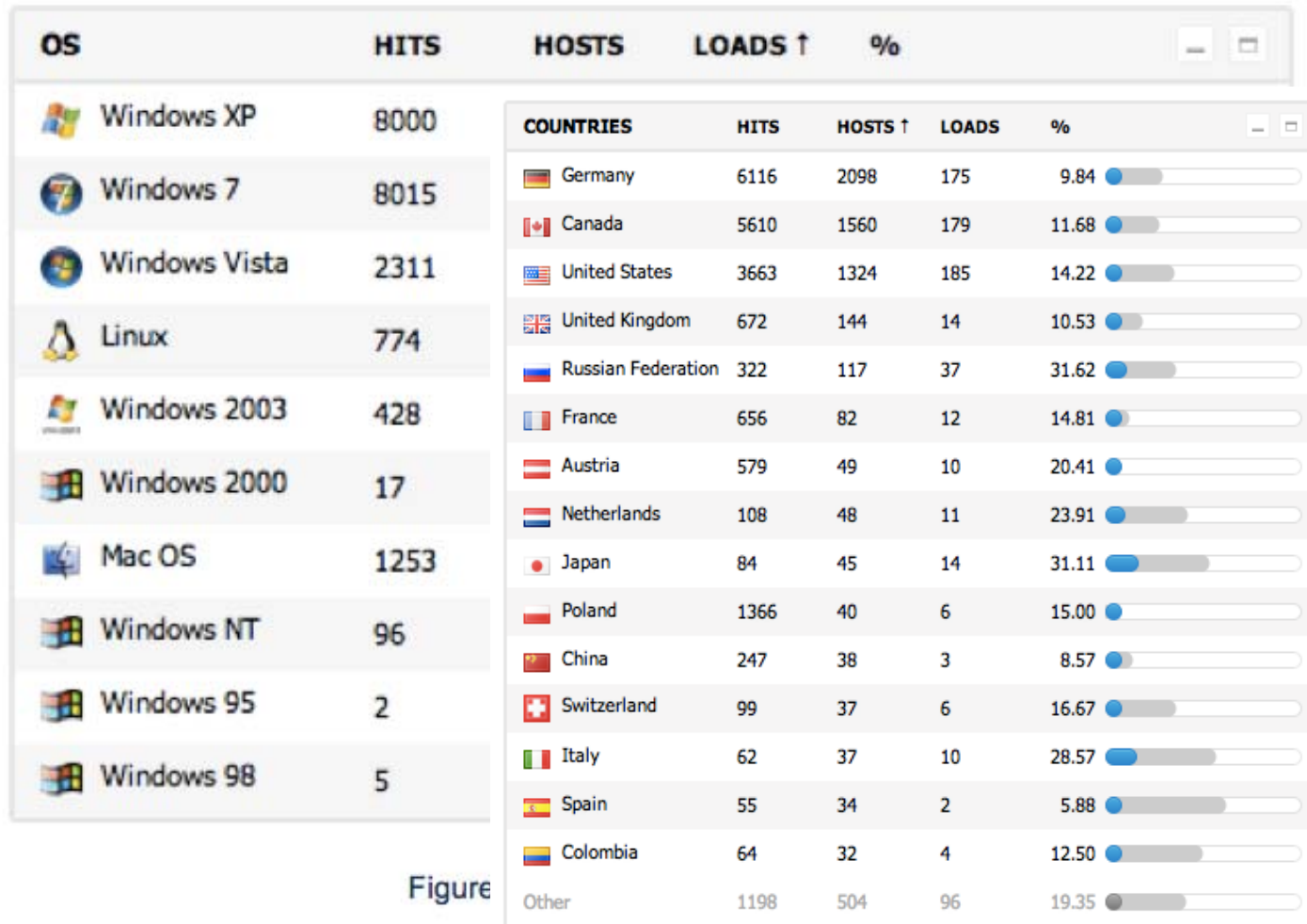Black hats are as sophisticated as white hats, sometimes more so…

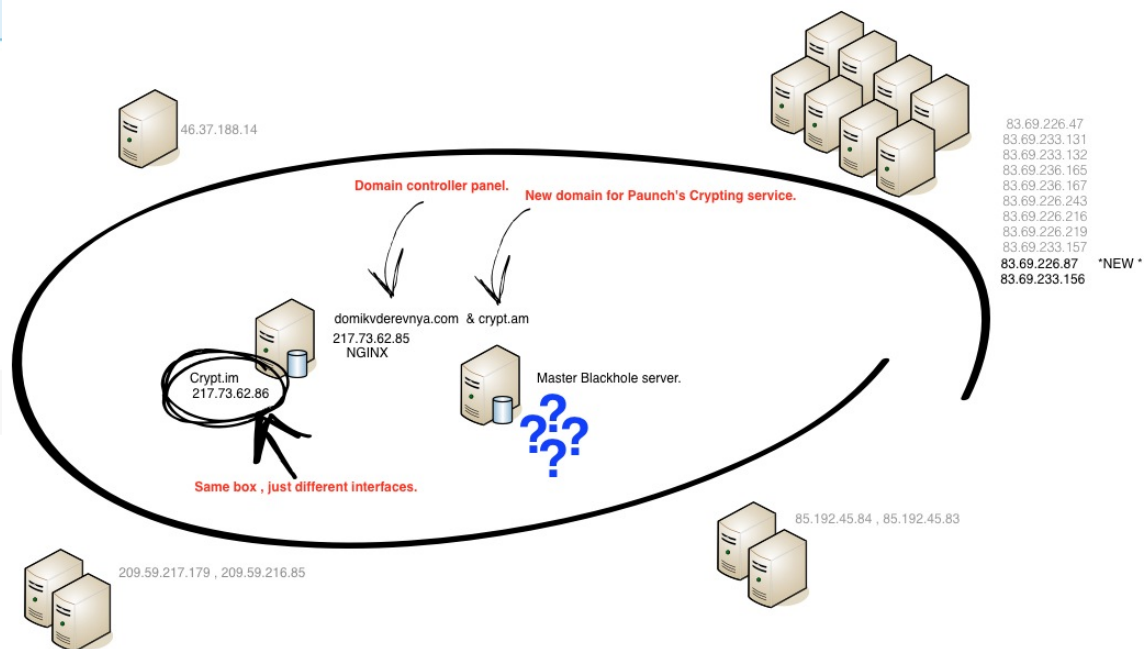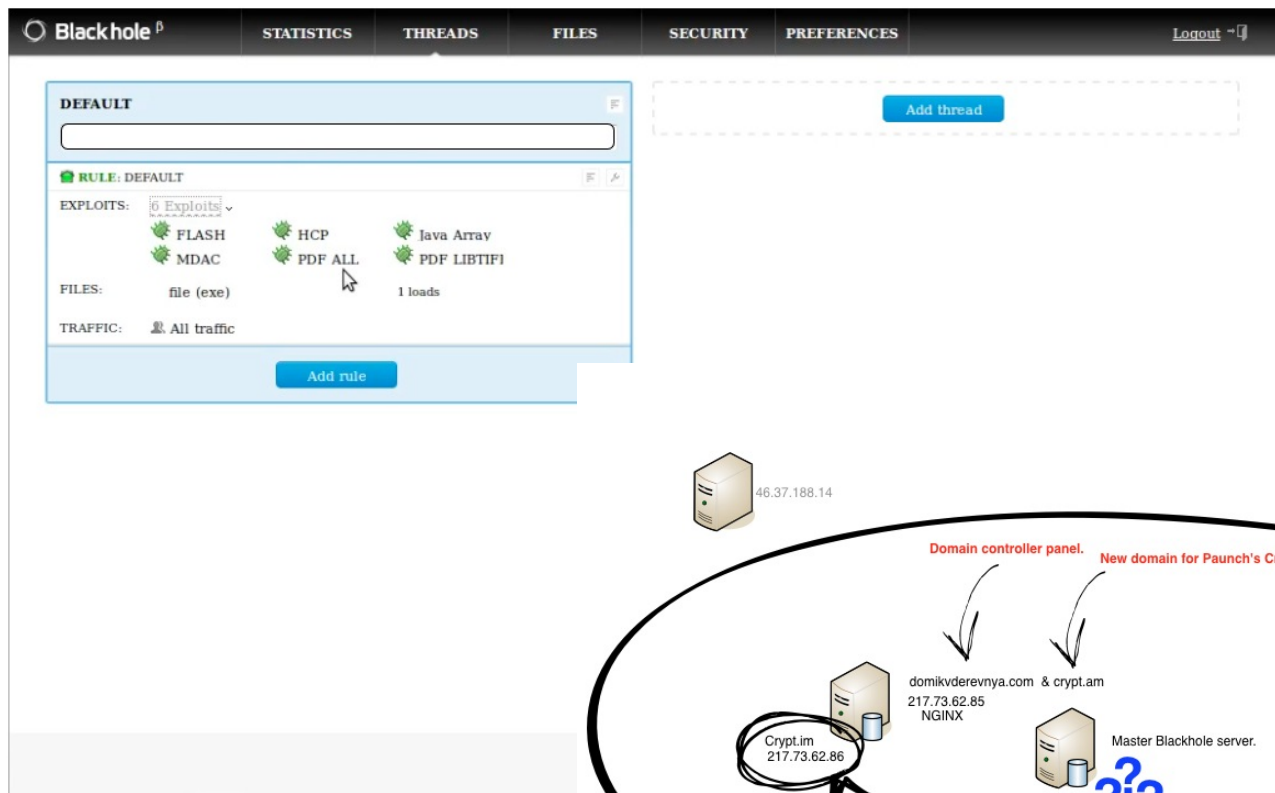Figure 6 Administrator Statistics page

BLACKHOLE EXPLOIT CONT.
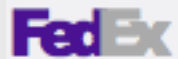
OS	HITS
Windows XP	8000
Windows 7	8015
Windows Vista	2311
Linux	774
Windows 2003	428
Windows 2000	17
Mac OS	1253
Windows NT	96
Windows 95	2
Windows 98	5

HOSTS   LOADS ↑   %

COUNTRIES	HITS	HOSTS ↑	LOADS	%
Germany	6116	2098	175	9.84
Canada	5610	1560	179	11.68
United States	3663	1324	185	14.22
United Kingdom	672	144	14	10.53
Russian Federation	322	117	37	31.62
France	656	82	12	14.81
Austria	579	49	10	20.41
Netherlands	108	48	11	23.91
Japan	84	45	14	31.11
Poland	1366	40	6	15.00
China	247	38	3	8.57
Switzerland	99	37	6	16.67
Italy	62	37	10	28.57
Spain	55	34	2	5.88
Colombia	64	32	4	12.50
Other	1198	504	96	19.35

Figure

- Buy outright
- Hosted
- Rent

The underground ecosystem is well developed and collaborative

From: LinkedIn Notification <innovatorswzz@ataportfoy.com.tr>   Hide
Subject: LinkedIn Nofitication service message
Date: October 11, 2012 6:56:23 AM PDT
To: info@internetidentity.com

LinkedIn

NOTIFICATIONS

Invitation notifications:

· From **Dillon Glover** (Your classmate)

PENDING NOTIFICATIONS

· There are a total of 3 letters awaiting your action. **Enter your InBox via this link.**

Don't wish to obtain email info letters? Change your letters settings.

LinkedIn values your privacy. Not once has LinkedIn made your email address open to any oth LinkedIn member without your permission. © 2010, LinkedIn Corporation.

IID

Welcome to UPS Team

You can use UPS Team to:

☐ Ship Online
☐ Schedule a Pickup
☐ Open a Your UPS Team Account

Dear, sales @ internetidentity.com.

Dear Client , RECIPIENT'S ADDRESS IS WRONG

Please print out the invoice copy attached and collect the package at our department.

With best regards , UPS Customer Services.

Copyright 2011 United Parcel Service of America, Inc. Your USPS TEAM, the United States Postal Services brandmark, and the color brown are trademarks of United Parcel Service of America, Inc. All rights reserved.

Please do not reply directly to this e-mail. USPS .US will not receive any reply message. For questions or comments, visit Contact UPS.

We understand the importance of privacy to our customers. For more information, please consult the Your USPS .COM Privacy Policy.

This communication contains proprietary information and may be confidential. If you are not the intended recipient, the reading, copying, disclosure or other use of the contents of this e-mail is strictly prohibited and you are instructed to please delete this e-mail immediately.

MyUps_id52....zip (70 KB)
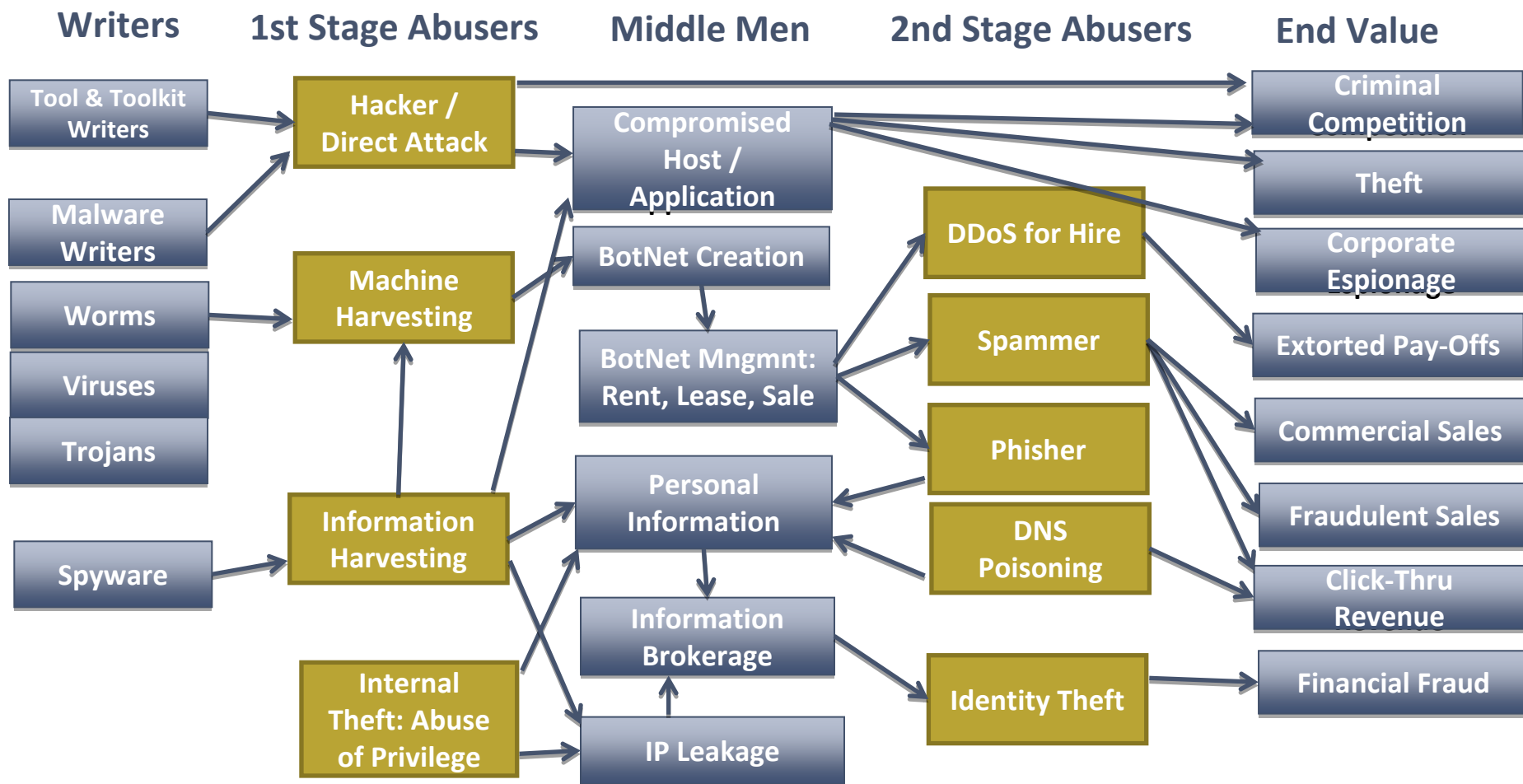
Negative consequences can be significant…

- Stolen / lost revenue

- Exfiltration of intellectual property

- Erosion of BRAND

- Disruption of network uptime

- Degraded IT reputation

- And the *most* important loss…

Loss of shareholder value

If something happens at your organization, the first question you'll ask is, "Is it just me or is everybody else getting hit with this attack?" You can't answer that for yourself…You've got to be part of a larger gene pool to get an immediate answer…

— *Renee Guttman, Chief Information Security Officer, The Coca Cola Company*
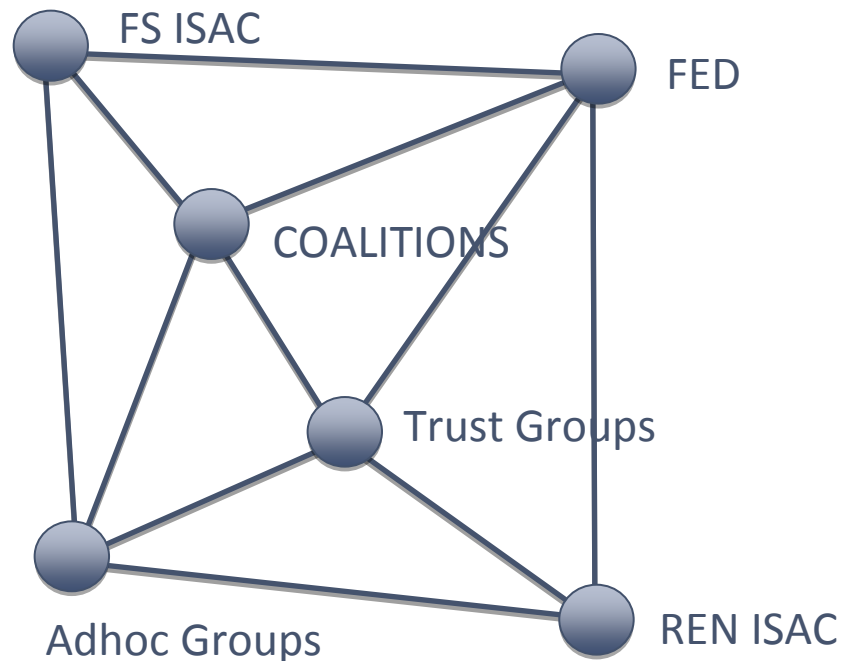
Collaboration is critical…

The issue of botnets is larger than any one industry or country. This is why partnership is so important

—*Howard Schmidt, former White House Cybersecurity Coordinator*

The new model needs to adapt to today's volume and velocity of information

FS ISAC

FED

COALITIONS

Trust Groups

Adhoc Groups

REN ISAC

SCALE your efforts beyond current known contacts - if were hit, chances are you're not alone

+

Extend your **Reach** beyond your own island of trust – collaboration can lead to new insights and learnings
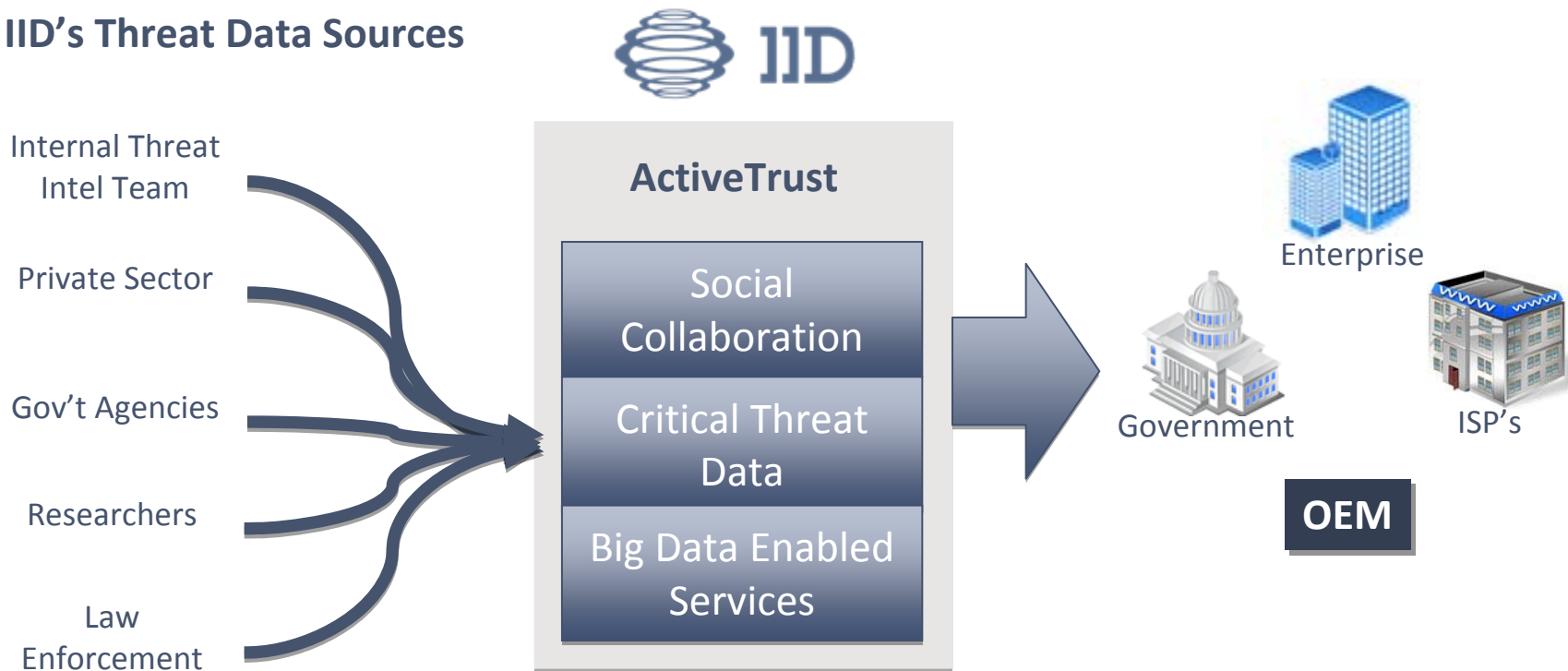
+

Leveraging a network to access actionable information faster leads to increased **EFFICACY**

We don't need another trust group

Information collection, exchange and analytics to produce the best actionable intelligence for the cybersecurity industry

IID's Threat Data Sources

Sources:
- Internal Threat Intel Team
- Private Sector
- Gov't Agencies
- Researchers
- Law Enforcement

ActiveTrust
- Social Collaboration
- Critical Threat Data
- Big Data Enabled Services

Outputs:
- Enterprise
- Government
- ISP's
- **OEM**

Thank you

Questions?

www.internetidentity.com